Vérificateur général
de la Ville de Québec

Audit de la gouvernance de la sécurité de l'information : bâtir la bonne stratégie d'audit

Daniel Rancourt, CPA auditeur, CA

VILLE DE QUÉBEC
l'accent d'Amérique

PRÉSENTATION

- Vérificateur général de la Ville de Québec
- Planification, portée et stratégie
- Résultats

VILLE DE QUÉBEC
l'accent d'Amérique

VÉRIFICATEUR GÉNÉRAL

LOI SUR LES CITÉS ET VILLES

- Municipalité de 100 000 habitants et plus
- Nommé et relève du conseil municipal
- Budget de fonctionnement minimum
- Responsable de l'application des politiques et normes
- Champs de compétence
- Droit
- Immunité

VÉRIFICATEUR GÉNÉRAL

VILLE DE QUÉBEC

- Équipe
- Audit réalisé annuellement
- Ligne de signalement

PLANIFICATION, PORTÉE ET STRATÉGIE

POINTS PARTICULIERS DE LA PLANIFICATION

- Qui sont les utilisateurs?
- Qu'est-ce qui est important?
- Compétence de l'équipe

PLANIFICATION, PORTÉE ET STRATÉGIE

OBJECTIF

- Déterminer dans quelle mesure la Direction de la Ville voit à la mise en place des assises nécessaires à une saine gouvernance et à la gestion de la sécurité de l'information et en surveille le fonctionnement.

PLANIFICATION, PORTÉE ET STRATÉGIE

CRITÈRES

- Attentes de la direction
- Catégorisation de l'information et désignation de détenteurs
- Gestion des risques
- Système de gestion de la sécurité de l'information numérique
- Processus et dispositifs de sécurité
- Sensibilisation et formation des utilisateurs et responsables
- Exercer la surveillance nécessaire

PLANIFICATION, PORTÉE ET STRATÉGIE

STRATÉGIE

- Approche d'audit générale
  - Approche corroborative
  - Absence de contrôle de gouvernance
- Approche d'audit détaillée
  - Exploitation des bases de données
  - Sélection d'actifs informationnels
  - Analyse particulière de quatre dispositifs de sécurité

RÉSULTATS

CONCLUSION GÉNÉRALE

- La Direction de la Ville n'a pas mis en place toutes les assises nécessaires à une gestion appropriée de la sécurité de l'information et elle n'effectue pas une surveillance suffisante.
- Observation : l'adoption d'une politique intégrée de sécurité de l'information est prévue au plan d'action pour la gestion de la sécurité de l'information depuis 2014; elle n'était toujours pas adoptée en mars 2017. Le vérificateur général a déjà formulé une recommandation en ce sens en 2012.
- Cette gouvernance expose la Ville à des risques, telles la divulgation de renseignements confidentiels, l'altération et la perte d'informations, l'interruption momentanée de ses systèmes informatiques et la discontinuité de ses opérations.

RÉSULTATS

CATÉGORISATION DE L'INFORMATION ET DÉSIGNATION DE DÉTENTEURS

- Beaucoup de systèmes d'information ont une cote « très élevée » en ce qui a trait à l'incidence d'une perte de disponibilité (95 sur 522, soit 18 %), ce qui est surprenant.
- Aucun détenteur n'a été désigné pour 105 des 522 systèmes d'information (20 %), dont ceux relatifs à 5 systèmes critiques.
- Une importante opération ponctuelle de catégorisation est actuellement en cours, alors que la catégorisation devrait se faire sur une base continue.

RÉSULTATS

GESTION DES RISQUES

- Le Service des technologies de l'information (STI) a pris quelques initiatives en vue de cibler les risques de sécurité de l'information. Toutefois, elles ne permettent pas de gérer l'ensemble des risques, puisqu'elles ont une portée limitée (ex. : opération pour déceler les risques liés à la désuétude des actifs informationnels).

RÉSULTATS

SYSTÈME DE GESTION DE LA SÉCURITÉ DE L'INFORMATION NUMÉRIQUE

- Un projet de cadre opérationnel de gestion, élaboré en 2013, étaye chacune des fonctions de l'équipe de sécurité, mais il n'a pas été approuvé par la Direction.
- L'équipe du STI n'est pas impliquée dans la gestion de certains volets de sécurité de l'information, tels les systèmes de contrôle industriels.
- La Ville n'a pas une vision claire des composantes physiques et logiques de sécurité à mettre en place.
- La planification de la sécurité de l'information numérique n'est pas suffisamment rigoureuse, de sorte que des actions importantes n'ont pas été réalisées ou n'ont été réalisées qu'en partie (ex. : sensibilisation et soutien à la continuité des activités).

RÉSULTATS

PROCESSUS ET DISPOSITIFS DE SÉCURITÉ

- La Direction n'a pas déployé suffisamment d'efforts pour orienter et soutenir la mise en œuvre des mesures de sécurité; elle reçoit peu d'informations sur la nature, le fonctionnement et l'efficacité de ces mesures.
- En 2015, environ 700 000 $ avait été prévu pour améliorer la gestion des accès. En 2016, l'engagement financier avait été amputé et ne s'élevait plus qu'à 150 000 $.

RÉSULTATS

CAPACITÉ À SOUTENIR LA CONTINUITÉ DES ACTIVITÉS

- Le STI ne dispose pas de l'information nécessaire pour produire le plan de continuité des services liés aux technologies de l'information.
  - Les plans de continuité des différentes unités administratives ne sont pas finalisés et un arbitrage n'a pas été réalisé pour assurer l'intégration des besoins et leur cohérence.
  - Comme les TI sont essentielles à la continuité de plusieurs services municipaux, le STI doit tenir compte des besoins liés à ces services dans son plan de continuité.
- Le STI n'a pas de plan d'intervention pour faire face à des risques particuliers, tels que les cyberattaques.

RÉSULTATS

GESTION DES INCIDENTS

- Les procédures pour réagir aux incidents sont peu élaborées.
- Il y a peu d'informations de consignées sur la nature des incidents.
- Les utilisateurs ne sont pas sensibilisés au fait qu'ils doivent signaler les incidents.
- Il n'y a pas d'analyse des incidents dans une perspective d'amélioration continue des dispositifs de sécurité.
- Aucune information n'est fournie sur la preuve à recueillir pour soutenir une action judiciaire ou disciplinaire.

RÉSULTATS

ÉVALUATION DE LA SÉCURITÉ DE L'INFORMATION

- Au cours des dernières années, la Ville a réalisé 29 analyses de vulnérabilité et tests d'intrusion. Parmi les problèmes décelés, mentionnons :
  - il n'y a pas de portait complet des suites données aux problèmes décelés;
  - les dossiers indiquent que les problèmes décelés n'ont été corrigés que pour 8 des 29 analyses ou tests effectués.

RÉSULTATS

SÉCURITÉ EXERCÉE SUR LES SYSTÈMES DE CONTRÔLE INDUSTRIELS

- La Ville a commencé à se préoccuper de la sécurité liée aux systèmes de contrôle industriels, mais peu de gestes ont été posés pour contenir les risques qui y sont associés :
  - il n'y a pas d'orientations communes pour l'informatisation de ces équipements;
  - aucune analyse complète des risques n'a été réalisée;
  - l'équipe de sécurité n'a pas été sollicitée pour proposer des mesures de sécurité;
  - il n'y a pas eu d'évaluation de l'efficacité des mesures de sécurité.

RÉSULTATS

ASSISES DE SÉCURITÉ EN PLACE

- Pour huit systèmes, nous avons voulu savoir si les assises étaient en place. Les principales faiblesses relevées sont :
  - une fiche de catégorisation n'existait que pour quatre de ces actifs;
  - un dossier de sécurité faisant état des mesures pour assurer une protection appropriée était constitué pour seulement quatre actifs;
  - une analyse de sécurité n'a été menée que pour un actif.

RÉSULTATS

SENSIBILISATION ET FORMATION DES UTILISATEURS ET RESPONSABLES

- Quelques actions de sensibilisation à la sécurité de l'information ont été menées, mais dans l'ensemble, peu d'efforts ont été déployés pour instaurer une culture à cet égard.
- Environ 700 des 6 000 employés ayant accès au système ont été invités à participer à des activités de sensibilisation.
  - Ainsi, la participation à une formation en ligne a été faible et six mois après la fin, aucun bilan n'a été effectué et aucune démarche n'a été entreprise pour l'étendre à l'ensemble du personnel.
- Six des huit employés qui ont des responsabilités dans la gestion des mesures de sécurité n'ont bénéficié d'aucune formation dans le domaine pour parfaire leur connaissance.

RÉSULTATS

ANALYSE DE LA GOUVERNANCE EXERCÉE SUR LA SÉCURITÉ DE L'INFORMATION

- L'implication de la Direction doit être renforcée.
- Les responsabilités d'acteurs essentiels au regard de la sécurité de l'information ne sont pas précisées.
- Il n'y a pas d'instance pour orienter les actions de l'ensemble des acteurs impliqués dans la gestion de la sécurité.
- La Direction n'exerce pas une surveillance adéquate et très peu d'informations de gestion lui sont transmises.

CONCLUSION

VILLE DE QUÉBEC
l'accent d'Amérique

MERCI!

QUESTIONS?

VILLE DE QUÉBEC
l'accent d'Amérique